EXHIBIT 449

Automotive News

June 12, 2019 02:39 PM

Hacker gained access to customer data at 130 dealerships, FTC says

JACKIE CHARNIGA □ □ □

DealerBuilt, an Iowa dealership software provider, reached a settlement with the Federal Trade Commission Wednesday over a 2016 breach of customer data that allowed a hacker to gain access to the personal information of about 12.5 million consumers stored by 130 dealership clients.

Editor's note: An earlier version of this article incorrectly stated that failure to encrypt data violated federal rule.

DealerBuilt, an Iowa dealership software provider, reached a settlement with the Federal Trade Commission Wednesday over a 2016 breach of customer data that allowed a hacker to gain access to the personal information of about 12.5 million consumers stored by 130 dealership clients.

The dealership management system provider agreed to a settlement with the FTC over the attack and will "take steps to better protect the data it collects," the FTC said.

The agency said in a statement that LightYear Dealer Technologies, known commercially as DealerBuilt, failed to properly encrypt sensitive data and conduct necessary vulnerability and penetration testing.

DealerBuilt CEO Michael Trasatti said Wednesday the company took immediate action when the breach occurred in 2016 and worked with customers. “We take securing customer data seriously,” Trasatti said in a statement. “We work to continuously improve our security.”

The breach will be resolved with a final consent agreement, which won't be made public unless it is accepted by the FTC. As part of the proposed consent agreement, DealerBuilt is required to implement a security program in accordance with the Safeguards Rule, and is prohibited from handling consumer data until the program is in place.

The settlement also requires the company to obtain third-party assessments of its security program every two years.

The FTC does not have authority to seek monetary penalties for an initial violation, but if the company violates the settlement, the commission could seek civil penalties of up to $42,530 per violation.

According to the complaint, DealerBuilt failed to protect the sensitive customer data, despite those resources being "readily available and relatively low-cost" to the provider. DealerBuilt sells dealership management systems and data processing systems.

Detected by dealer

The breach, which occurred over 10 days, took place in DealerBuilt's backup database beginning in late October 2016.

"The hacker downloaded the personal information of more than 69,000 consumers, including their Social Security numbers, driver's license numbers, and birthdates, as well as wage and financial information," the FTC said in the statement.

In the complaint, the FTC said the hacker attacked DealerBuilt's system "multiple times, downloading the personal information of 69,283 consumers, the entire backup directories of five customers."

The breach was detected by a DealerBuilt auto dealer customer, who had found customers' data online.

"The settlement with DealerBuilt imposes more specific security requirements and requires company executives to take more responsibility for order compliance, while also strengthening the third party assessor's accountability and providing the FTC with additional tools for oversight," FTC Chairman Joe Simons said in the statement.

Safeguards Rule violation

The FTC alleges that the data DealerBuilt collected was stored and transmitted in clear text. Though neglecting to encrypt data is not yet a direct violation of the Gramm-Leach-Bliley Act's Safeguards Rule, the FTC considered not doing so was a failure to implement basic safeguards, which ultimately led to the breach. Data also was stored without access controls or authentication protections, also deemed necessary under the rule.

The FTC considers DealerBuilt's activities an example of unfair practices.

DMS systems typically store private and public consumer data, including but not limited to names, addresses, birth dates, credit information and Social Security numbers. The software also contains similarly sensitive information about dealership employees, such as payroll data and bank account information, according to the statement.

The complaint also alleges that a DealerBuilt employee "connected a storage device to the company's backup network without ensuring that it was securely configured, leaving an insecure connection for 18 months."

Additionally, the FTC alleges DealerBuilt never conducted vulnerability or penetration testing; drafting, implementing or maintaining a written security policy; or provided training for employees.

Inline Play

Source URL: *https://www.autonews.com/dealers/hacker-gained-access-customer-data-130-dealerships-ftc-says*